

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-153227

(43)Date of publication of application : 23.05.2003

(51)Int.Cl.

H04N 7/167
G06K 19/00
G06K 19/10
H04H 1/00
H04L 9/08
H04L 9/18
H04N 5/44
H04N 7/173

(21)Application number : 2001-347641

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 13.11.2001

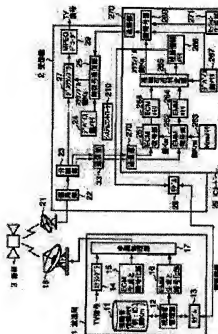
(72)Inventor : OI SHINICHI

(54) BROADCAST RECEPTION PROCESSING SYSTEM, BROADCAST RECEPTION PROCESSING METHOD AND IC CARD APPLIED TO RECEPTION APPARATUS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an IC card the illegal use of which can be prevented by using only a reception apparatus of a particular model for target.

SOLUTION: The IC card applied to the reception apparatus for receiving scrambled broadcast programs, is provided with: a communication means (270) that makes communication with the reception apparatus and a transmission control means (265) that particularizes a type of a device key possessed by the reception apparatus and transmits a session key encrypted by the device key and a scramble key encrypted by the session key to the reception apparatus so long as it is cleared that the reception apparatus is not the particular model on the basis of the particularization.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-153227

(P2003-153227A)

(43) 公開日 平成15年5月23日 (2003. 5. 23)

(51) Int.Cl. ⁷	識別記号	F I	テ-グ-ト ⁷ (参考)
H 0 4 N	7/167	H 0 4 H 1/00	F 5 B 0 3 5
G 0 6 K	19/00	H 0 4 N 5/44	Z 5 C 0 2 5
	19/10		6 4 0 A 5 C 0 6 4
H 0 4 H	1/00		Z 5 J 1 0 4
H 0 4 L	9/08	H 0 4 L 9/00	6 0 1 B

審査請求 有 請求項の数11 O L (全 21 頁) 最終頁に続く

(21) 出願番号 特願2001-347641(P2001-347641)

(71) 出願人 000003078

(22) 出願日 平成13年11月13日 (2001. 11. 13)

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 大井 伸一

神奈川県横浜市中区新杉田町8番地 株

式会社東芝横浜事業所内

(74) 代理人 100058479

弁理士 鈴木 武彦 (外6名)

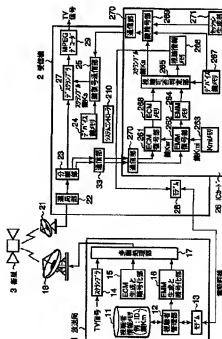
最終頁に続く

(54) 【発明の名称】 放送受信処理システム、放送受信処理方法、及び受信装置に適用されるICカード

(57) 【要約】

【課題】 特定機種種の受信装置だけをターゲットにして不正を防止することが可能なICカードを提供すること。

【解決手段】 スクランプル放送を受信する受信装置に適用されるICカードであって、受信装置と通信する通信手段(270)と、受信装置が保持するデバイス鍵の種類を特定し、この特定の結果に基づき受信装置が特定機種種に該当しないことが判明したときに限り、受信装置に対してデバイス鍵で暗号化したセッション鍵、及びセッション鍵で暗号化したスクランブル鍵を送信する送信制御手段(265)とを備えている。



【特許請求の範囲】

【請求項1】 ICカード、及びこのICカードを受け付けて放送波を受信する受信装置を含む放送受信処理システムであって、

前記受信装置は、

放送波を受信する放送受信手段と、

暗号化された復号鍵を復号化するためのデバイス鍵を記憶する記憶手段と、

前記ICカードと通信する第1の通信手段と、

前記第1の通信手段を介して暗号化された復号鍵を受信し、この暗号化された復号鍵を前記記憶手段に記憶されたデバイス鍵により復号化する第1の復号手段と、

前記第1の通信手段を介して放送波のスクランブルを解除するための暗号化されたスクランブル鍵を受信し、前記第1の復号手段により復号化された復号鍵により暗号化されたスクランブル鍵を復号化する第2の復号手段と、

前記第2の復号手段により復号化されたスクランブル鍵により、前記放送受信手段により受信される放送波のスクランブルを解除するスクランブル解除手段と、

を備え、

前記ICカードは、

前記受信装置と通信する第2の通信手段と、

復号鍵を生成する復号鍵生成手段と、

デバイス鍵により復号鍵を暗号化する第1の暗号手段と、

復号鍵によりスクランブル鍵を暗号化する第2の暗号手段と、

前記第2の通信手段を介して前記放送受信手段により受信された放送波に含まれる鍵識別情報を受け取り、この鍵識別情報に基づき前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当しないことが判明したとき、前記第2の通信手段により暗号化された復号鍵及び暗号化されたスクランブル鍵を送信し、前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したとき、前記第2の通信手段による暗号化された復号鍵の送信を禁止する送信制御手段と、
を備えたことを特徴とする放送受信処理システム。

【請求項2】 ICカード、及びこのICカードを受け付けて放送波を受信する受信装置を含む放送受信処理システムであって、

前記受信装置は、

放送波を受信する放送受信手段と、

暗号化された復号鍵を復号化するためのデバイス鍵を記憶する記憶手段と、前記ICカードと通信する第1の通信手段と、

前記第1の通信手段を介して暗号化された復号鍵を受信し、この暗号化された復号鍵を前記記憶手段に記憶されたデバイス鍵により復号化する第1の復号手段と、

前記第1の通信手段を介して放送波のスクランブルを解

除するための暗号化されたスクランブル鍵を受信し、前記第1の復号手段により復号化された復号鍵により暗号化されたスクランブル鍵を復号化する第2の復号手段と、

前記第2の復号手段により復号化されたスクランブル鍵により、前記放送受信手段により受信される放送波のスクランブルを解除するスクランブル解除手段と、

前記第1の通信手段を介してメッセージ出力制御情報を受信したとき、前記放送波に含まれる所定のメッセージを出力する出力手段と、

を備え、

前記ICカードは、

前記受信装置と通信する第2の通信手段と、

復号鍵を生成する復号鍵生成手段と、

デバイス鍵により復号鍵を暗号化する第1の暗号手段と、

復号鍵によりスクランブル鍵を暗号化する第2の暗号手段と、

前記第2の通信手段を介して前記放送受信手段により受信された放送波に含まれる鍵識別情報を受け取り、この鍵識別情報に基づき前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当しないことが判明したとき、前記第2の通信手段により暗号化された復号鍵及び暗号化されたスクランブル鍵を送信し、前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したとき、前記第2の通信手段を介してメッセージ出力制御情報を送信する送信制御手段と、
を備えたことを特徴とする放送受信処理システム。

【請求項3】 前記ICカードは、

前記第2の通信手段を介して前記放送受信手段により受信された放送波に含まれる復号鍵送信制御情報を受け取り、前記鍵識別情報に基づき前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したときであって、前記復号鍵送信制御情報により復号鍵の送信が指示されているときには、前記第2の通信手段により暗号化された復号鍵を送信し、前記復号鍵送信制御情報により復号鍵の否送信が指示されているときには、前記第2の通信手段による暗号化された復号鍵の送信を禁止する復号鍵送信制御手段、

を備えたことを特徴とする請求項2に記載の放送受信処理システム。

【請求項4】 ICカード、及びこのICカードを受け付けて放送波を受信する受信装置を含む放送受信処理システムであって、

前記受信装置は、

放送波を受信する放送受信手段と、

暗号化された復号鍵を復号化するためのデバイス鍵を記憶する記憶手段と、

前記ICカードと通信する第1の通信手段と、

前記第1の通信手段を介して暗号化された復号鍵を受信

し、この暗号化された復号鍵を前記記憶手段に記憶されたデバイス鍵により復号化する第1の復号手段と、
前記第1の通信手段を介して放送波のスクランブルを解除するための暗号化されたスクランブル鍵を受信し、前記第1の復号手段により復号化された復号鍵により暗号化されたスクランブル鍵を復号化する第2の復号手段と、
前記第2の復号手段により復号化されたスクランブル鍵により、前記放送受信手段により受信される放送波のスクランブルを解除するスクランブル解除手段と、
前記第1の通信手段を介してメッセージ出力の指示を受信したとき、前記放送波に含まれる所定のメッセージを出力する出力手段と、
を備え、
前記ICカードは、
前記受信装置と通信する第2の通信手段と、
復号鍵を生成する復号鍵生成手段と、
デバイス鍵により復号鍵を暗号化する第1の暗号手段と、
復号鍵によりスクランブル鍵を暗号化する第2の暗号手段と、
前記第2の通信手段を介して前記放送受信手段により受信された放送波に含まれる鍵識別情報を受け取り、この鍵識別情報に基づき前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当しないことが判明したとき、前記第2の通信手段により暗号化された復号鍵及び暗号化されたスクランブル鍵を送信する第1の送信制御手段と、
前記第2の通信手段を介して前記放送受信手段により受信された放送波に含まれる復号鍵送信制御情報を受け取り、前記鍵識別情報に基づき前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したときであって、前記復号鍵送信制御情報により復号鍵の送信が指示されているときには、前記第2の通信手段により暗号化された復号鍵を送信し、前記復号鍵送信制御情報により復号鍵の否送信が指示されているときには、前記第2の通信手段による暗号化された復号鍵の送信を禁止する第2の送信制御手段と、
前記第2の通信手段を介して前記放送受信手段により受信された放送波に含まれるメッセージ出力制御情報を受け取り、前記鍵識別情報に基づき前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したときであって、前記メッセージ出力制御情報によりメッセージの出力が指示されているときには、前記第2の通信手段によりメッセージ出力の指示を送信し、前記メッセージ出力制御情報によりメッセージの否出力が指示されているときには、前記第2の通信手段によるメッセージ出力の指示の送信を禁止する第3の送信制御手段と、
を備えたことを特徴とする放送受信処理システム。

【請求項5】前記放送波は、暗号化された番組情報を含み、
前記番組情報は、暗号化された前記鍵識別情報及び前記スクランブル鍵を含む、
ことを特徴とする請求項1、2、3、又は4に記載の放送受信処理システム。
【請求項6】暗号化された復号鍵を復号化するためのデバイス鍵を記憶し、ICカードから暗号化された復号鍵及び暗号化されたスクランブル鍵を受信し、前記デバイス鍵により暗号化された復号鍵を復号化し、復号化された復号鍵により暗号化されたスクランブル鍵を復号化し、復号化されたスクランブル鍵により放送波のスクランブルを解除する受信装置に適用されるICカードであって、
前記受信装置と通信する通信手段と、
復号鍵を生成する復号鍵生成手段と、
デバイス鍵により復号鍵を暗号化する第1の暗号手段と、
復号鍵によりスクランブル鍵を暗号化する第2の暗号手段と、
前記通信手段を介して前記受信装置で受信された放送波に含まれる鍵識別情報を受け取り、この鍵識別情報に基づき前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当しないことが判明したとき、前記受信装置に対して前記通信手段より暗号化された復号鍵及び暗号化されたスクランブル鍵を送信し、前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したとき、前記受信装置に対して前記通信手段による暗号化された復号鍵の送信を禁止する送信制御手段と、
を備えたことを特徴とするICカード。
【請求項7】暗号化された復号鍵を復号化するためのデバイス鍵を記憶し、ICカードから暗号化された復号鍵及び暗号化されたスクランブル鍵を受信し、前記デバイス鍵により暗号化された復号鍵を復号化し、復号化された復号鍵により暗号化されたスクランブル鍵を復号化し、復号化されたスクランブル鍵により放送波のスクランブルを解除し、ICカードからメッセージ出力の指示を受信したとき、前記放送波に含まれる所定のメッセージを出力する受信装置に適用されるICカードであって、
前記受信装置と通信する通信手段と、
復号鍵を生成する復号鍵生成手段と、
デバイス鍵により復号鍵を暗号化する第1の暗号手段と、
復号鍵によりスクランブル鍵を暗号化する第2の暗号手段と、
前記通信手段を介して前記受信装置で受信された放送波に含まれる鍵識別情報を受け取り、この鍵識別情報に基づき前記受信装置に記憶されたデバイス鍵が所定のデバ

イス鍵に該当しないことが判明したとき、前記受信装置に対して前記通信手段により暗号化された復号鍵及び暗号化されたスクランブル鍵を送信し、前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したとき、前記受信装置に対して前記通信手段によりメッセージ出力制御情報を送信する送信制御手段と、
を備えたことを特徴とする IC カード。

【請求項 8】 前記通信手段を介して前記受信装置で受信された放送波に含まれる復号鍵送信制御情報を受け取り、前記鍵識別情報に基づき前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したときであって、前記復号鍵送信制御情報により復号鍵の送信が指示されているときには、前記受信装置に対して前記通信手段により暗号化された復号鍵及び暗号化されたスクランブル鍵を送信し、前記復号鍵送信制御情報により復号鍵の否送信が指示されているときには、前記受信装置に対して前記第 2 の通信手段による暗号化された復号鍵の送信を禁止する復号鍵送信制御手段を備えたことを特徴とする請求項 7 に記載の IC カード。

【請求項 9】 暗号化された復号鍵を復号化するためのデバイス鍵を記憶し、IC カードから暗号化された復号鍵及び暗号化されたスクランブル鍵を受信し、前記デバイス鍵により暗号化された復号鍵を復号化し、復号化された復号鍵により暗号化されたスクランブル鍵を復号化し、復号化されたスクランブル鍵により放送波のスクランブルを解除し、IC カードからメッセージ出力の指示を受信したとき、前記放送波に含まれる所定のメッセージを出力する受信装置に適用される IC カードであって、

前記受信装置と通信する通信手段と、
復号鍵を生成する復号鍵生成手段と、
デバイス鍵により復号鍵を暗号化する第 1 の暗号手段と、

復号鍵によりスクランブル鍵を暗号化する第 2 の暗号手段と、
前記通信手段を介して前記受信装置で受信された放送波に含まれる鍵識別情報を受け取り、この鍵識別情報に基づき前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当しないことが判明したとき、前記受信装置に対して前記通信手段により暗号化された復号鍵及び暗号化されたスクランブル鍵を送信する第 1 の送信制御手段と、

前記通信手段を介して前記受信装置で受信された放送波に含まれる復号鍵送信制御情報を受け取り、前記鍵識別情報に基づき前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したときであって、前記復号鍵送信制御情報により復号鍵の送信が指示されているときには、前記受信装置に対して前記通信手段により暗号化された復号鍵を送信し、前記復号鍵送信

制御情報により復号鍵の否送信が指示されているときには、前記受信装置に対して前記通信手段による暗号化された復号鍵の送信を禁止する第 2 の送信制御手段と、
前記通信手段を介して前記受信装置で受信された放送波に含まれるメッセージ出力制御情報を受け取り、前記鍵識別情報に基づき前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したときであって、前記メッセージ出力制御情報によりメッセージの出力が指示されているときには、前記受信装置に対して前記通信手段によりメッセージ出力の指示を送信し、前記メッセージ出力制御情報によりメッセージの否出力が指示されているときには、前記受信装置に対して前記通信手段によるメッセージ出力の指示の送信を禁止する第 3 の送信制御手段と、
を備えたことを特徴とする IC カード。

【請求項 10】 IC カードは、受信装置により受信された放送波に含まれる鍵識別情報に基づき、予め受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することを認識したとき、受信装置に対して予め記憶された

20 デバイス鍵で暗号化された復号鍵の送信を禁止し、
IC カードは、受信装置により受信された放送波に含まれる鍵識別情報に基づき、予め記憶されたデバイス鍵が所定のデバイス鍵に該当しないことを認識したとき、受信装置に対して予め記憶されたデバイス鍵で暗号化された復号鍵、及び復号鍵で暗号化されたスクランブル鍵を送信し、
受信装置は、暗号化された復号鍵及び暗号化されたスクランブル鍵を受信し、予め記憶されたデバイス鍵により暗号化された復号鍵を復号化し、この復号化された復号

30 鍵により暗号化されたスクランブル鍵を復号化し、この復号化されたスクランブル鍵により受信された放送波のスクランブルを解除する、
ことを特徴とする放送受信処理方法。

【請求項 11】 IC カードは、受信装置により受信された放送波に含まれる鍵識別情報に基づき、予め受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することを認識したとき、受信装置に対して予め記憶された

40 デバイス鍵で暗号化された復号鍵の送信を禁止し、
IC カードは、受信装置により受信された放送波に含まれる鍵識別情報に基づき、予め記憶されたデバイス鍵が所定のデバイス鍵に該当しないことを認識したとき、受信装置に対して予め記憶されたデバイス鍵で暗号化された復号鍵、及び復号鍵で暗号化されたスクランブル鍵を送信する、
ことを特徴とする放送受信処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、放送局から放送される放送波を受信し処理する放送受信処理システム及び放送受信処理方法に関する。また、この発明は、放送

局から放送される放送波を受信し処理する受信装置に適用されるＩＣカードに関する。

【０００２】

【従来の技術】放送局からのスクランブルされた放送を受信する受信装置は、スクランブル鍵によりスクランブルを解除して映像や音声を出力する。このスクランブル鍵は外部に漏洩しないように安全に管理されており、このスクランブル鍵を入手できる正規ユーザだけが、例えばスクランブルされた有料放送を視聴することができる。

【０００３】

【発明が解決しようとする課題】受信装置には様々な機種が存在する。しかし、特定機種の受信装置における不正が発覚しても、この特定機種の受信装置だけをターゲットにして不正を防止することはできない。不正が発覚した特定機種の受信装置が野放し状態になれば、有料放送事業者はそれなりのダメージを受けることになる。

【０００４】この発明の目的は、上記したような事情に鑑み成されたものであって、特定機種の受信装置だけをターゲットにして不正を防止することが可能な放送受信処理システム、放送受信処理方法、及び受信装置に適用されるＩＣカードを提供することにある。

【０００５】

【課題を解決するための手段】上記課題を解決し目的を達成するために、この発明の放送受信処理システム、放送受信処理方法、及び受信装置に適用されるＩＣカードは、以下のように構成されている。

【０００６】(１)この発明は、ＩＣカード、及びこのＩＣカードを受け付けて放送波を受信する受信装置を含む放送受信処理システムであって、前記受信装置は、放送波を受信する放送受信手段と、暗号化された復号鍵（＝セッション鍵）を復号化するためのデバイス鍵を記憶する記憶手段と、前記ＩＣカードと通信する第１の通信手段と、前記第１の通信手段を介して暗号化された復号鍵を受信し、この暗号化された復号鍵を前記記憶手段に記憶されたデバイス鍵により復号化する第１の復号手段と、前記第１の通信手段を介して放送波のスクランブルを解除するための暗号化されたスクランブル鍵を受信し、前記第１の復号手段により復号化された復号鍵により暗号化されたスクランブル鍵を復号化する第２の復号手段と、前記第２の復号手段により復号化されたスクランブル鍵により、前記放送受信手段により受信される放送波のスクランブルを解除するスクランブル解除手段と、を備え、前記ＩＣカードは、前記受信装置と通信する第２の通信手段と、復号鍵を生成する復号鍵生成手段と、デバイス鍵により復号鍵を暗号化する第１の暗号手段と、復号鍵によりスクランブル鍵を暗号化する第２の暗号手段と、前記第２の通信手段を介して前記放送受信手段により受信された放送波に含まれる鍵識別情報を受け取り、この鍵識別情報に基づき前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当しないことが

判明したとき、前記第２の通信手段により暗号化された復号鍵及び暗号化されたスクランブル鍵を送信し、前記記憶手段に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したとき、前記第２の通信手段による暗号化された復号鍵の送信を禁止する送信制御手段と、を備えている。

【０００７】(２)この発明は、暗号化された復号鍵（＝セッション鍵）を復号化するためのデバイス鍵を記憶し、ＩＣカードから暗号化された復号鍵及び暗号化されたスクランブル鍵を受信し、前記デバイス鍵により暗号化された復号鍵を復号化し、復号化された復号鍵により暗号化されたスクランブル鍵を復号化し、復号化されたスクランブル鍵により放送波のスクランブルを解除する受信装置に適用されるＩＣカードであって、前記受信装置と通信する通信手段と、復号鍵を生成する復号鍵生成手段と、デバイス鍵により復号鍵を暗号化する第１の暗号手段と、復号鍵によりスクランブル鍵を暗号化する第２の暗号手段と、前記通信手段を介して前記受信装置で受信された放送波に含まれる鍵識別情報を受け取り、この鍵識別情報に基づき前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当しないことが判明したとき、前記受信装置に対して前記通信手段により暗号化された復号鍵及び暗号化されたスクランブル鍵を送信し、前記受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することが判明したとき、前記受信装置に対して前記通信手段による暗号化された復号鍵の送信を禁止する送信制御手段と、を備えている。

【０００８】(３)この発明の放送受信処理方法は、ＩＣカードが、受信装置により受信された放送波に含まれる鍵識別情報に基づき、予め受信装置に記憶されたデバイス鍵が所定のデバイス鍵に該当することを認識したとき、受信装置に対して予め記憶されたデバイス鍵で暗号化された復号鍵の送信を禁止し、ＩＣカードが、受信装置により受信された放送波に含まれる鍵識別情報に基づき、予め記憶されたデバイス鍵が所定のデバイス鍵に該当しないことを認識したとき、受信装置に対して予め記憶されたデバイス鍵で暗号化された復号鍵、及び復号鍵で暗号化されたスクランブル鍵を送信し、受信装置が、暗号化された復号鍵及び暗号化されたスクランブル鍵を受信し、予め記憶されたデバイス鍵により暗号化された復号鍵を復号化し、この復号化された復号鍵により暗号化されたスクランブル鍵を復号化し、この復号化されたスクランブル鍵により受信された放送波のスクランブルを解除する。

【０００９】

【発明の実施の形態】以下、この発明の第１の実施形態について図面を参照して説明する。

【００１０】図１は、この発明の第１の実施形態に係る放送受信処理システムの基本構成を示す図である。図１に示すように、放送受信処理システムは、放送局１、受

信機 2、及び衛星 3 を備えている。

【0011】放送局 1 は、契約したものが視聴できるように有料放送番組の信号をスクランブル 14 にてスクランブル（暗号化）して放送する。番組をスクランブル（暗号化）する際に使用したスクランブル鍵 K s や番組の視聴条件に関する情報を含む番組情報（以下 ECM）を ECM 生成と暗号化部 15 にて生成し、多重処理部 17 にて番組に多重しアンテナ 18 から放送する。ECM は不正ができないように暗号化されており、暗号化に使用する鍵をワーク鍵 Kw と呼ぶ。一方、個々の視聴者に対しては視聴可能な期間や視聴可能なチャンネル、番組のタイプなど契約条件の情報、ECM を復号するために使用するワーク鍵 Kw を含む個別情報（以下 EMM）を EMM 生成と暗号化部 16 にて生成し、多重処理部 17 にて放送信号に多重しアンテナ 18 から放送する。この EMM も不正ができないようにマスター鍵 Km i にて暗号化する。暗号化に使用するマスター鍵 Km i は IC カード 26 の Km i メモリ 263 に記憶されている鍵であり、IC カード製造時もしくは発行時に書き込まれる情報である。

【0012】放送局 1 のアンテナ 18 から放送される放送波は、衛星 3 を介して、受信機 2 のアンテナ 21 で受信される。受信機 2 は、放送局 1 から送られてくる暗号化された EMM を分離部 23 にて分離する。分離された EMM は、受信機 2 の通信部 33 を介して、IC カード 26 内の通信部 270 に送信される。通信部 270 で受信された EMM は、IC カード 26 内の EMM 復号部 262 に送られる。EMM 復号部 262 は、Km i メモリ 263 に記憶されているマスター鍵 Km i を用いて暗号化された EMM を復号し、EMM メモリ 264 に記憶する。復号された EMM に含まれるワーク鍵 Kw は、ECM 復号部 261 に提供される。一方、受信機 2 は、放送局 1 から送られてくる暗号化された ECM も分離部 23 にて分離する。分離された ECM は、受信機 2 の通信部 33 を介して、IC カード 26 内の通信部 270 に送信される。通信部 270 で受信された ECM は、IC カード 26 内の ECM 復号部 261 に送られる。ECM 復号部 261 は、ワーク鍵 Kw を用いて暗号化された ECM を復号し、ECM メモリ 268 に一時的に記憶する。視聴可否判定部 265 は、ECM 及び EMM を使用して視聴可否判定を下し、契約している番組（もしくはチャンネル）が視聴できる場合には、ECM から番組をデスクランブル（復号化）するためのスクランブル鍵 K s を取り出して、デスクランブラ 27 を制御し視聴する。なお、スクランブル鍵 K s が通常数行程度の間隔で更新されるたびに、ECM は更新される。

【0013】IC カード 26 と受信機 2 とは、共有のデバイス鍵を有する。IC カード 26 は、受信機 2 に対して、共有のデバイス鍵を使用してスクランブル鍵を暗号化して出力する。受信機 2 は、共有のデバイス鍵を使用

して暗号化されたスクランブル鍵を復号化する。これにより、IC カード 26 と受信機 2 のインターフェース上に生データのスクランブル鍵を露出しない様にする。ここで、鍵の暗号化及び復号化について具体的に説明する。デバイス鍵メモリ 267 に格納されている複数のデバイス鍵のうち、対象の受信機 2 に格納されているデバイス鍵と同じデバイス鍵が、鍵暗号部 269 に入力される。さらに、ECM メモリ 268 に格納された ECM に含まれるスクランブル鍵が、鍵暗号部 269 に入力される。

10 鍵暗号部 269 は、デバイス鍵によりスクランブル鍵を暗号化する。暗号化されたスクランブル鍵は、通信部 270 を介して受信機 2 に入力される。受信機 2 は、鍵復号通信部 25 を介して、暗号化されたスクランブル鍵を受信する。鍵復号通信部 25 は、デバイス鍵メモリ 264 から供給されるデバイス鍵により、暗号化されたスクランブル鍵を復号し、復号されたスクランブル鍵をデスクランブラ 27 に供給する。デスクランブラ 27 は、供給されたスクランブル鍵により放送のスクランブルを解除する。

20 【0014】IC カード 26 では、ペーパービュー（以下 P P V）と呼ばれる番組ごとに購入、非購入を選択できる放送方式に対応するため、視聴情報メモリ 266 を持っている。視聴者がペーパービュー番組を選択し、購入を決めた場合には、IC カード 26 は当該ペーパービュー番組の ECM 内にある番組を特定するための情報（視聴情報）を IC カード内の視聴情報メモリ 266 に記憶すると共に、デスクランブラを制御し視聴できるようにする。この視聴情報は、電話回線（モデム 28 及びモデム 13）を通じて放送局 1 に回収され、視聴料の精算を行うようになっている。回収された視聴情報は、視聴者管理部 12 を介して視聴者情報メモリ 11 に格納される。

【0015】図 2～図 8 は、図 1 で説明した放送受信処理システムにおいて、特定機種を不正装置（不良受信機）だけをターゲットにして不正を防止する不正防止処理を説明するための図である。

【0016】図 2 に示すように、有料放送信号は受信機 1 に入力され、視聴者が選択した（選局部 22 にて選局した）番組が視聴契約があり視聴可能な場合にはデスクランブラ 27 にてデスクランブル処理された後、M P E G デコーダ 29 の処理を経て受信機 2 から出力される。この処理の中で視聴契約があるか否かの判断は IC カード 26 が行っており、具体的には有料放送信号に多重されている ECM を分離部 23 にて分離し、IC カード 26 へ入力した後、IC カード 26 が当該 ECM を使用して視聴契約があるか否かの判断をする。

【0017】視聴契約があると IC カード 26 が判断した場合に、IC カード 26 は有料放送信号をデスクランブルするためのスクランブル K s 鍵を、IC カード 26 内のデバイス鍵メモリ 267 にて記憶しているデバイ

11

ス鍵にて暗号化した後、受信機 2へ与える。なお、I Cカード 26 内での暗号化処理は I Cカード 26 内の図示しないマイクロプロセッサにてソフト処理で行うことも可能であれば、I Cカード 26 内に暗号化処理用の専用ハードウェアを有して処理することも可能である。

【0018】次に、デバイス鍵にて暗号化されたスクランブル鍵 K s を受けた受信機 2 では、I Cカード 26 と同様、予めデバイス鍵メモリ 24 に記憶しているデバイス鍵を用いて復号後送信部 25 にて復号化し、スクランブル鍵 K s を得て、希望する番組をデスクランブルするものである。

【0019】以上の説明で I Cカード 26 は、I Cカード 26 が挿入される可能性のあるすべての受信機のデバイス鍵およびその識別情報を予め記憶しているものほか、E CM等を使用して放送局からデバイス鍵およびその識別情報を設定できるものとしている。またデバイス鍵は、例えば受信機メーカー毎、機種毎、あるいは受信機毎に異なるものとする。例えば図 2 では全部で 8 種類の受信機、すなわちデバイス鍵に対応しているもので、メーカー毎に異なる場合に相当する程度のデバイス鍵の種類である。デバイス鍵メモリ 26 7 には、全部で 8 種類のデバイス鍵を記憶しており、例えば受信機 2 がデバイス鍵識別 = 3 の受信機であれば、I Cカード 26 はデバイス鍵識別 = 3 のデバイス鍵を使用して暗号化処理をおこなうものとしている。

【0020】次に不良受信機の特定について説明する。放送局 1 では、例えば不良受信機のデバイス鍵識別ごとの良否表を E CMに多重して送る。この良否表を含む E CMを受信した I Cカード 26 は当該表をメモリ 26 8 にて記憶し、以後不良と示されているデバイス鍵識別のデバイス鍵を有する受信機とは暗号通信をしないように動作する。ここで不良受信機のデバイス鍵識別の良否表を E CMに多重することとしたのは、E CMは有料放送のスクランブルされた番組を視聴する際にスクランブル鍵を得るために必須の情報であり、不良受信機を所有する人が不良受信機のデバイス鍵識別の良否表を I Cカード 26 に与えないように不正しようとしても、番組を視聴するためには E CMを入力せざるをえないため、不正に対する抑止力となることからである。

【0021】図 2 の例ではデバイス鍵識別 = 3 が不良であり、このデバイス鍵識別 = 3 が割り付けられている受信機 1 とは、I Cカード 26 は暗号通信をしない。すなわち、I Cカード 26 は暗号化したスクランブル鍵 K s を与えないのである。なお受信機 2 が、制限されない例えばデバイス鍵識別 = 1 の受信機のふりをしたとしても、図 2 の例でいえば受信機 2 はデバイス鍵識別 = 3 のデバイス鍵しか記憶していない。このため、I Cカード 26 によりデバイス鍵識別 = 1 のデバイス鍵で暗号化されたスクランブル鍵 K s を受信機 1 が受けても、復号できずデスクランブルは不可能である。

12

【0022】次に、I Cカード 26 が受信機 2 のデバイス鍵識別を取得する方法について説明する。電源 on 後に、受信機 2 と I Cカード 26 において初期化通信処理が行われるが、このときに I Cカード 26 が受信機 2 のデバイス鍵識別を取得することとする。また、E CMを受信機 2 から I Cカード 26 へ入力する際に、E CMにデバイス鍵識別を付加することにより I Cカード 26 が取得することも可能である。

【0023】また上記説明では、不良受信機のデバイス鍵識別の良否表は E CMに多重して送信されるものとしたが、この送信方法に限定されるものではなく放送局から I Cカードに対して安全に送信できればよい。つまり、E CMを暗号化するワーク鍵 K w 以外の I Cカード 26 と放送局間で共有化されている情報にて暗号化され送られるものであれば、E CM以外でもよい。例えば放送波に多重され I Cカード 26 に入力される E CM以外の情報であってもよいし、PPV 放送を受信する場合にあっては、I Cカード 26 に蓄積した PPV の視聴情報を、放送局側にアップロードする際暗号通信を行うが、その通信の際にデバイス鍵識別の良否表を放送局側からダウンロードし、得てよい。

【0024】次に、図 3 を参照して、図 1 で説明した放送受信処理システムにおいて特定機種の受信装置だけをターゲットにして不正を防止する不正防止処理の別例について説明する。図 3 は、不正防止のために排除すべきデバイス鍵識別のみ送付するケースを示す図である。このように、排除すべきデバイス鍵識別のみ送付するようにしても、図 2 で説明したケースと同様の効果を得ることができる。図 2 の例は、デバイス鍵識別 = 3 の受信機を制限する例であって、I Cカードはデバイス鍵識別 = 3 という情報をメモリ 26 8 に記憶するものである。

【0025】さらに制限する受信機が生じた場合には、放送側から追加で制限すべき受信機のデバイス鍵識別が送信され、I Cカードのメモリ 26 8 に追加記憶していくようになる。また逆に問題であった受信機がバージョンアップ等で制限が不要となった場合には、放送側から制限を解除すべき受信機のデバイス鍵識別が送信され、I Cカード 26 ではメモリ 26 8 に当該デバイス鍵識別があった場合にはメモリ 26 8 から削除するものである。

【0026】図 2 及び図 3 に示す例では、暗号処理をすべてデバイス鍵にて行う例を示したが、暗号通信においては、電源 on 後に受信機 1 と I Cカード 26 において、デバイス鍵を使用した暗号通信により相互認証を行うとともに、相互認証が問題なかった場合に以後の暗号通信に使用するテンポラリなセッション鍵を共有化し、スクランブル鍵の暗号化処理は、このセッション鍵を使用し行うという場合もある。この場合には I Cカード 26 において、相互認証処理時に、受信機 1 のデバイス鍵識別の良否判定を行い、不良と判断する場合には相

13

互認証をエラー終了とし、受信機1に通知するとともに、以後1カード26はスクランブル鍵を与えないというようにしても良い。なお、後で、第2の実施形態として、セッション鍵を利用するケースについて説明する。

【0027】続いて、図4を参照して、図2及び図3の受信機に対してデバイス鍵識別の良否を示す情報を送信する送信局1について説明する。基本的な動作は図1で説明した通りである。

【0028】図4に示すように、入力信号はスクランブラ14にてスクランブルされた後、多重処理部17に入力される。ECM生成と暗号化部15の中のECM生成部15aは、ECMを生成する。ここで生成されるECMには、スクランブル鍵Ks、番組の視聴条件に関する情報、及びデバイス鍵識別の良否を示す情報が含まれる。番組の視聴条件に関する情報は、受信機2に挿入される1カード26にて視聴条件の判定を行うための番組情報(例えば、放送年月日時分秒情報、番組の課金方法(ペイパービュー番組、ティア契約番組)を示す情報など、視聴の可否を判定し、料金等の視聴条件を提示するための情報である。生成されたECMは、ECM生成と暗号化部15の中の暗号化部15bにて暗号化される。暗号化されたECMは、多重処理部17に入力される。なお、暗号化部15bは、ワーク鍵Kwにて暗号化処理を行う。このワーク鍵Kwは、視聴者が放送局と視聴契約をした場合に放送局から与えられる鍵情報であり、EMMによって各受信機2の1カード26に与えられる。なお、ワーク鍵Kwは1カード26を配布する。もしくは受信機2と一緒に販売される際に予め1カード26内に記憶されている場合もある。

【0029】視聴者管理部12は、視聴者情報メモリ11に格納された各視聴者の視聴契約の有無を示す情報を読み出す。EMM生成と暗号化部16の中のEMM生成部16aは、視聴者管理部12より読み出された情報に従い、個々の受信機2の1カード26に対して、視聴を許可するもしくは禁止するための契約情報を含むEMMを生成する。EMM生成と暗号化部16の中の暗号化部16bは、生成されたEMMを暗号化する。暗号化されたEMMは多重処理部17に入力される。なお暗号化部16bは、マスター鍵Km1にて暗号化処理を行う。このマスター鍵Km1は、各1カード26に固有の鍵である。このマスター鍵Km1は1カード製造、発行時に1カード26に書き込まれ、放送側で管理している情報である。

【0030】上記図4に示す放送局1と図2又は図3に示す受信機2とを組み合わせて放送サービスが提供される。これにより、放送局側から不正が行われている特定機種の受信機を指定し、有料放送を受信する不良受信機を排除することができる。

【0031】次に、図5を参照して、図1で説明した放

14

送受信処理システムにおいて、特定機種を受信装置(不良受信機)だけをターゲットにして、メッセージを通知するメッセージ通知処理を説明する。図5は、受信機2及び1カード26の概略構成を示す図である。図5に示す受信機2及び1カード26の基本構成は、図1に示す受信機2及び1カード26と同じである。但し、図5に示すように、この受信機2には、画像若しくは音声信号への変換部31及び多重処理部32が追加されている。

【0032】不良受信機の特定方法は、図2で説明した不良受信機のデバイス鍵識別の良否表をECMに多重して送信する方法、又は図3で説明した不良受信機のデバイス鍵識別のみをECMに多重して送信する方法が採用されるものとする。

【0033】図5において、放送側から不良受信機を特定するためのデバイス鍵識別に関する情報、及び当該デバイス鍵識別を有する受信機に表示すべきメッセージの番号を示す情報が送信される。これら情報は、受信機2により受信され、1カード26に提供される。1カード26は、ECMメモリ268にこれら情報を記憶する。1カード26は、不良と示されているデバイス鍵識別のデバイス鍵を有する受信機に対しメッセージの番号を通知する。

【0034】図5の例ではデバイス鍵識別=3の受信機2と接続された1カード26は、当該受信機のデバイス鍵識別をECMメモリ268に記憶しており、ECMメモリ268に記憶しているメッセージの番号を受信機に通知し、受信機に表示させるように要求する。

【0035】メッセージの番号の通知を受けた受信機2は、分離部23により要求されたメッセージの番号のメッセージを分離する。このデータは、例えばメッセージ表示するためのキャラクタデータであり、得られたメッセージ情報を画像若しくは音声信号への変換部31によりTV画面表示するための画像信号に変換し、多重処理部32によりオンスクリーン表示するための多重処理がなされる。なお、ここでは一例としてキャラクタを画面にオンスクリーン表示する例を説明したが、音声や画像であってもよく、ポイントとなるのは放送局が特定機種の不良受信機に対し表示すべきメッセージを指定できるという点である。これにより個々の受信機に対して「修理を促す」、「連絡先を通知する」など異なるメッセージを通知し、所有者に知らせることができる。以上説明したメッセージの伝送に関しては、例えばデジタル放送の番組配列情報に配置し、伝送すればよい。

【0036】次に、図6を参照して、図5に示す受信機2に対しデバイス鍵識別の良否を示す情報を多重しながら放送を行うケースについて説明する。図6は、送信局1の概略構成を示す図である。図6に示す送信局1の基本構成は、図1に示す放送局1と同じである。但し、図6に示すように、この送信局1には、メッセージ生成部

19が追加されている。

【0037】図6に示すように、入力信号はスクランブル14によりスクランブルされた後、多重処理部17に入力される。ECM生成と暗号化部15の中のECM生成部15aは、ECMを生成する。ここで生成されるECMには、スクランブル鍵Ks、番組の視聴条件に関する情報、及びデバイス鍵識別の良否を示す情報が含まれる。番組の視聴条件に関する情報は、受信機2に挿入されるICカード26にて視聴条件の判定を行うための番組情報（例えば、放送年月日時分秒情報、番組の課金方法（ペーパービュー番組、ティア契約番組）を示す情報など、視聴の可否を判定し、料金等の視聴条件を提示するための情報である。生成されたECMは、ECM生成と暗号化部15の中の暗号化部15bにて暗号化される。暗号化されたECMは、多重処理部17に入力される。なお、暗号化部15bは、ワーク鍵Kwにて暗号化処理を行う。このワーク鍵Kwは、視聴者が放送局と視聴契約をした場合に放送局から与えられる鍵情報であり、EMMによって各受信機2のICカード26に与えられる。なお、ワーク鍵KwはICカード26を配布する、もしくは受信機2と一緒に販売される際に予めICカード26内に記憶されている場合もある。

【0038】視聴者管理部12は、視聴者情報メモリ11に格納された各視聴者の視聴契約の有無を示す情報を読み出す。EMM生成と暗号化部16の中のEMM生成部16aは、視聴者管理部12により読み出された情報に従い、個々の受信機2のICカード26に対して、視聴を許可するもしくは禁止するための契約情報を含むEMMを生成する。EMM生成と暗号化部16の中の暗号化部16bは、生成されたEMMを暗号化する。暗号化されたEMMは多重処理部17に入力される。なお暗号化部16bは、マスター鍵Km1にて暗号化処理を行う。このマスター鍵Km1は、各ICカード26に固有の鍵である。このマスター鍵Km1はICカード製造、発行時にICカード26に書き込まれ、放送側で管理している情報である。

【0039】さらにメッセージ生成部19は、メッセージ番号と、このメッセージ番号で表示すべき情報、例えばキャラクターデータ等を対にした情報を生成し、多重処理部17に入力する。

【0040】この図6に示す送信局1と図5に示す受信機2とを組み合わせる放送サービスを提供することにより、放送局側から不正が行われている受信機を指定し、有料放送を受信する不良受信機に対して例えば機種ごとに異なるメッセージを表示せしめることが可能となる。

【0041】前述の例では、不良受信機に対して、暗号通信を禁止し、スクランブル鍵Ksの供給を停止する、もしくはメッセージを表示させることを放送局が指定した。次に、図7及び図8を参照して、暗号通信の禁止、及びメッセージの表示の両方を選択的に放送局が指定可

能な例について説明する。

【0042】図7に示す送信局1の基本構成は、図6に示す送信局1と同じである。但し、図7に示すように、ECM生成部15aの人力として、メッセージ表示の有無を示す情報、及び暗号通信の禁止の有無を示す情報の二つの情報が追加される。放送局1の運用としては不良受信機に対して、（1）暗号通信を禁止し、さらにメッセージを表示させる様に指定する場合、（2）暗号通信を禁止し、メッセージを表示しない様に指定する場合（図2、図3、図4で説明した不正防止処理と同様）、（3）暗号通信を禁止せず、メッセージを表示させる様に指定する場合（図5、図6で説明した不正防止処理と同様）、（4）暗号通信を禁止せず、メッセージも表示しない様に指定する場合、の4通りで運用できる。

【0043】図8は、図7に示す送信局1から送信される放送波を受信する受信機2及びICカード26の一例を示す図である。この図8に示す受信機2及びICカード26の基本構成は、図5に示す受信機2及びICカード26と同じである。異なるのは、図8に示すICカード26は、ECMメモリ268内に暗号通信の禁止の有無を示す情報、及びメッセージ表示の有無を示す情報の二つの情報を記憶する点である。これら二つの情報は、ECMの一部としてICカード26に入力される。不良受信機に対しては、これら二つの情報に従い、暗号通信及び表示指示が制御される。

【0044】例えば、図8の例では、ECMメモリ268に、メッセージ表示＝有り、暗号通信禁止＝無し、デバイス鍵識別＝3の受信機に対してメッセージ番号＝3のメッセージを表示する、が記憶されるとする。つまり、ICカード26は受信機2に対して、これら情報を送信する。これら情報を受信した受信機2は、メッセージ番号＝3のメッセージを放送信号から分離し、画像もしくは音声信号への変換部31にて表示画面を生成し、多重処理部32にてTV信号に多重する。

【0045】この図8の例では、メッセージ表示＝有り、暗号通信禁止＝無しであり、当該受信機が不良受信機に指定されている、あるいはサービスセンターに連絡が必要などのメッセージ表示がなされる。しかしながら、暗号通信は禁止されておらず、契約があればスクランブル放送の視聴は可能である。メッセージ表示＝有り、暗号通信禁止＝有り、すなわち、メッセージ表示をおこない、さらに暗号通信を禁止し、視聴不可とすることが可能である。

【0046】このように、放送側からメッセージ表示情報と暗号通信禁情報とをそれぞれ設定することにより、不良受信機に対する不正防止処理の自由度を広げることができる。

【0047】次に、図9～図11に示すフローチャートを参照して、この発明の不正防止処理をまとめる。

【0048】図9は、特定機種の受信機だけをターゲット

トにして、ＩＣカードとの暗号通信を禁止する不正防止処理を説明するフローチャートである。

【００４９】放送局１が、デバイス鍵鑑別の良否を示す情報を含むＥＣＭを生成し暗号化する（ＳＴ１１）。暗号化されたＥＣＭは、ＴＶ信号に多重して放送される（ＳＴ１２）。受信機２は、放送局１からの放送波を受信する（ＳＴ１３）。受信した放送波から暗号化されたＥＣＭを分離する（ＳＴ１４）。分離されたＥＣＭは、受信機２の通信部３３及びＩＣカード２６の通信部２７

０を介して、ＩＣカードに提供される（ＳＴ１５）。ＩＣカードは、暗号化されたＥＣＭを復号化し、デバイス鍵鑑別の良否を示す情報を得る（ＳＴ１６）。このとき、ＩＣカードの視聴可否判定部２６５は、デバイス鍵鑑別の良否を示す情報をＩＣカード内に記憶するとともに、この良否を示す情報に基づき、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当するか否かを判断する（ＳＴ１７）。視聴可否判定部２６５により、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当しないと判断されると（ＳＴ１８、

ＮＯ）、ＩＣカードは受信機と通信を行い、ＩＣカードから受信機に対して暗号化されたスクランブル鍵を送信する（ＳＴ１９）。視聴可否判定部２６５により、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当すると判断されると（ＳＴ１８、ＹＥＳ）、ＩＣカードは受信機との通信を禁止する（ＳＴ２０）。つまり、ＩＣカードから受信機に対してデバイス鍵により暗号化されたスクランブル鍵は送信されない。

【００５０】図１０は、特定機種種の受信機だけをターゲットにして、所定のメッセージの表示を指示する不正防止処理を説明するフローチャートである。

【００５１】放送局１が、デバイス鍵鑑別の良否を示す情報及びメッセージの番号を含むＥＣＭを生成し暗号化する（ＳＴ３１）。暗号化されたＥＣＭは、ＴＶ信号に多重して放送される（ＳＴ３２）。受信機２は、放送局１からの放送波を受信する（ＳＴ３３）。受信した放送波から暗号化されたＥＣＭを分離する（ＳＴ３４）。分離されたＥＣＭは、受信機２の通信部３３及びＩＣカード２６の通信部２７０を介して、ＩＣカードに提供される（ＳＴ３５）。ＩＣカードは、暗号化されたＥＣＭを復号化し、デバイス鍵鑑別の良否を示す情報を得る（ＳＴ３６）。このとき、ＩＣカードの視聴可否判定部２６５は、デバイス鍵鑑別の良否を示す情報をＩＣカード内に記憶するとともに、この良否を示す情報に基づき、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当するか否かを判断する（ＳＴ３７）。視聴可否判定部２６５により、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当すると判断されると（ＳＴ３８、ＹＥＳ）、ＩＣカードは受信機に対して、所定のメッセージの表示を指示するためのメッセージの

番号を送信する（ＳＴ４０）。このメッセージの番号の送信を受けた受信機は、このメッセージの番号に対応するメッセージを放送波から抽出し、抽出したメッセージを出力する（ＳＴ４１）。視聴可否判定部２６５により、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当しないと判断されると（ＳＴ３８、ＮＯ）、ＩＣカードから受信機に対して、メッセージの番号は送信されない（ＳＴ３９）。

【００５２】図１１は、特定機種種の受信機だけをターゲットにして、ＩＣカードとの暗号通信を選択的に禁止したり、選択的に所定のメッセージを表示させたりする不正防止処理を説明するフローチャートである。

【００５３】放送局１が、デバイス鍵鑑別の良否を示す情報、メッセージの番号、暗号通信を禁止するか否かを制御する第１の制御情報、及びメッセージを表示するか否かを制御する第２の制御情報を含むＥＣＭを生成し暗号化する（ＳＴ５１）。暗号化されたＥＣＭは、ＴＶ信号に多重して放送される（ＳＴ５２）。受信機２は、放送局１からの放送波を受信する（ＳＴ５３）。受信した放送波から暗号化されたＥＣＭを分離する（ＳＴ５

４）。分離されたＥＣＭは、受信機２の通信部３３及びＩＣカード２６の通信部２７０を介して、ＩＣカードに提供される（ＳＴ５５）。ＩＣカードは、暗号化されたＥＣＭを復号化し、デバイス鍵鑑別の良否を示す情報を得る（ＳＴ５６）。このとき、ＩＣカードの視聴可否判定部２６５は、デバイス鍵鑑別の良否を示す情報をＩＣカード内に記憶するとともに、この良否を示す情報に基づき、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当するか否かを判断する（ＳＴ５７）。

視聴可否判定部２６５により、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当しないと判断されると（ＳＴ５８、ＮＯ）、ＩＣカードは受信機と通信を行い、ＩＣカードから受信機に対してデバイス鍵により暗号化されたスクランブル鍵を送信する（ＳＴ５９）。視聴可否判定部２６５により、受信機に記憶されたデバイス鍵が、ターゲットのデバイス鍵に該当すると判断されると（ＳＴ５８、ＹＥＳ）、第１の制御情報に基づきＩＣカードとの暗号通信が選択的に禁止されたり、第２の制御情報に基づき選択的に所定のメッセージが表示されたりする（ＳＴ６０）。具体的に言うと、第１の制御情報により暗号通信が禁止されていればＩＣカードと受信機との間の暗号通信は禁止される。第２の制御情報により所定のメッセージの表示が指示されていればＩＣカードから受信機に対してメッセージの番号は通知されない。

【００５４】次に、この発明の第２の実施形態について

図面を参照して説明する。この第2の実施形態は、先に説明した第1の実施形態の応用例である。従って、第1の実施形態と重複する内容についての説明は省略する。

【0055】図12は、この発明の第2の実施形態に係る放送受信処理システムの基本構成を示す図である。図13～図15は、図12で説明した放送受信処理システムにおいて、特定機能の受信装置（不良受信機）だけをターゲットにして不正を防止する不正防止処理を説明するための図である。図13に示す不正防止処理は図3に示す不正防止処理に対応し、図14に示す不正防止処理は図5に示す不正防止処理に対応し、図15に示す不正防止処理は図8に示す不正防止処理に対応する。以下、図1、図3、図5、及び図8に示す放送受信処理システムと異なる箇所を中心に、図12～図15に示す放送受信処理システムを説明する。

【0056】まず、受信機1とICカード2は暗号通信により相互認証を行い、相互認証が問題ない場合にICカード2から受信機1へテンポラリなセッション鍵が与えられる。このテンポラリなセッション鍵は、今回の相互認証においてICカード2が生成した鍵であり、次の相互認証においてはICカード2は別の鍵を生成するものである。

【0057】まず始めに受信機1からICカード2に対しデバイス鍵識別番号を示す。ICカード2ではこれまで受信していたECMにおいて、当該受信機が不良であることをしめすデバイス鍵識別番号が送付されておらず、ICカード2内のメモリ268内に当該受信機が不良であることをしめす情報がない場合には、テンポラリなセッション鍵をセッション鍵生成部271にて生成し、当該受信機のデバイス鍵にて暗号化し、受信機1へ渡す。なおセッション鍵生成部271は暗号器や乱数生成器等を使用し、同じセッション鍵が生成されないようになっているものである。このようにセッション鍵はデバイス鍵にて暗号化されることから正しいデバイス鍵を持つ受信機以外にはセッション鍵が渡ることなく、また相互認証を行うたびに毎回変わることから、前回取得した鍵を流用することもできない。このため、第1の実施形態で説明したように、デバイス鍵でスクランブル鍵の暗号化処理を行う場合に比べ安全性が高い。セッション鍵を受信機2とICカード26で共有化した以降に、ECMを受信した受信機1はECMをICカード26に与え、レスポンスでセッション鍵にて暗号化されたスクランブル鍵を得て、これを鍵復号通信部25bにて復号し、デスクランブラ27へ与えるものである。なおECM内には適宜放送局から不良なデバイスを示すデバイス鍵識別が送られており、これを受信したICカード26ではメモリ268内に記憶し、以後の相互認証において記憶したデバイス鍵識別を利用した暗号通信を行わず、セッション鍵の共有化を行わないように処理するものである。また逆に問題であった受信機2がバージョンアップ

等で制限が不要となった場合には、放送側から制限を解除すべき受信機のデバイス鍵識別が送信され、ICカード2ではメモリ268に当該デバイス鍵識別があった場合にはメモリ268から削除するものである。

【0058】例えば、受信機2において、相互認証（セッション鍵の復号化処理）は鍵復号通信部25aで処理され、スクランブル鍵の復号化処理は鍵復号通信部25bで処理される。又は、暗号アルゴリズムが同じ場合には、鍵を切り替える構成となっていればよく、相互認証とスクランブル鍵の復号化処理を共通化することもできる。

【0059】ここで、鍵の暗号化処理及び復号化処理についてまとめる。つまり、ICカード26により、このICカード26が装填された受信機2が排除対象の受信機に該当しないことが判明したときの処理についてまとめる。

【0060】図12に示すように、ICカード26は、セッション鍵生成部271を備えている。このセッション鍵生成部271により生成されるセッション鍵は、鍵暗号部269に入力される。また、デバイス鍵メモリ267に記憶されている複数のデバイス鍵のうち、対象の受信機2に格納されているデバイス鍵と同じデバイス鍵が、鍵暗号部269に入力される。さらに、ECMメモリ268に格納されたECMに含まれるスクランブル鍵が、鍵暗号部269に入力される。

【0061】鍵暗号部269は、デバイス鍵によりセッション鍵を暗号化し、セッション鍵によりスクランブル鍵を暗号化する。鍵暗号部269により暗号化されたセッション鍵及び暗号化されたスクランブル鍵は、通信部270を介して受信機2に入力される。受信機2は、鍵復号通信部25を介して、暗号化されたセッション鍵及び暗号化されたスクランブル鍵を受信する。なお、鍵復号通信部25の一部が図13に示す鍵復号通信部25aに相当し、同様に、鍵復号通信部25の一部が図13に示す鍵復号通信部25bに相当する。

【0062】鍵復号通信部25は、デバイス鍵メモリ24から供給されるデバイス鍵により、暗号化されたセッション鍵を復号する。さらに、鍵復号通信部25は、復号されたセッション鍵により暗号化されたスクランブル鍵を復号し、復号されたスクランブル鍵をデスクランブラ27に供給する。デスクランブラ27は、供給されたスクランブル鍵により放送のスクランブルを解除する。

【0063】次に、図14を参照して、図12で説明した放送受信処理システムにおいて、特定機能の受信装置（不良受信機）だけをターゲットにして、メッセージを通知するメッセージ通知処理を説明する。図14は、受信機2及びICカード26の略略構成を示す図である。図14に示す受信機2及びICカード26の基本構成は、図12に示す受信機2及びICカード26と同じである。但し、図14に示すように、この受信機2には、

21

画像若しくは音声信号への変換部31及び多重処理部32が追加されない。

【0064】不良受信機の特定方法は、図2で説明した不良受信機のデバイス鍵識別の良否表をECMに多重して送信する方法、又は図3（或いは図13）で説明した不良受信機のデバイス鍵識別のみをECMに多重して送信する方法が採用されるものとする。

【0065】図14において、放送側から不良受信機を特定するためのデバイス鍵識別に関する情報、及び当該デバイス鍵識別を有する受信機に表示すべきメッセージの番号を示す情報が送信される。これら情報は、受信機2により受信され、ICカード26に提供される。ICカード26は、ECMメモリ268にこれら情報を記憶する。ICカード26は、不良と示されているデバイス鍵識別のデバイス鍵を有する受信機に対しメッセージ出力制御情報を通知する。メッセージ出力制御情報とは、例えばメッセージの番号である。

【0066】図14の例ではデバイス鍵識別=3の受信機2と接続されたICカード26は、当該受信機のデバイス鍵識別をECMメモリ268に記憶しており、ECMメモリ268に記憶しているメッセージの番号を受信機に通知し、受信機に表示させるように要求する。

【0067】メッセージの番号の通知を受けた受信機2は、分離部23により要求されたメッセージの番号のメッセージを分離する。このデータは、例えばメッセージ表示するためのキャラクタデータであり、得られたメッセージ情報を画像若しくは音声信号への変換部31によりTV画面表示するための画像信号に変換し、多重処理部32によりオンスクリーン表示するための多重処理がなされる。なお、ここでは一例としてキャラクタを画面にオンスクリーン表示する例を説明したが、音声や画像であってもよく、ポイントとなるのは放送局が特定機種の不良受信機に対し表示すべきメッセージを指定できるという点である。これにより個々の受信機に対して「修理を促す」、「連絡先を通知する」など異なるメッセージを通知し、所有者に知らしめることができる。以上説明したメッセージの伝送に関しては、例えばデジタル放送の番組配列情報に配置し、伝送すればよい。

【0068】前述の例では、不良受信機に対して、暗号通信を禁止し、スクランブル鍵Ksの供給を停止する、もしくはメッセージを表示させることを放送局が指定した。次に、図15を参照して、暗号通信の禁止（暗号化されたセッション鍵及び暗号化されたスクランブル鍵の非送信）、及びメッセージの表示（メッセージ出力制御情報の送信）の両方を選択的に放送局が指定可能な例について説明する。

【0069】放送局1の運用としては不良受信機に対して、（1）暗号通信を禁止し、さらにメッセージを表示させる様に指定する場合、（2）暗号通信を禁止し、メッセージを表示しない様に指定する場合、（3）暗号通

22

信を禁止せず、メッセージを表示させる様に指定する場合、（4）暗号通信を禁止せず、メッセージも表示しない様に指定する場合、の4通りで運用できる。

【0070】図15は、送信局1から送信される放送波を受信する受信機2及びICカード26の一例を示す図である。この図15に示す受信機2及びICカード26の基本構成は、図14に示す受信機2及びICカード26と同じである。異なるのは、図15に示すICカード26は、ECMメモリ268内に暗号通信の禁止の有無を示す情報、及びメッセージ表示の有無を示す情報の二つの情報を記憶する点である。これら二つの情報は、ECMの一部としてICカード26に入力される。不良受信機に対しては、これら二つの情報に従い、暗号通信及び表示指示が制御される。

【0071】例えば、図15の例では、ECMメモリ268に、メッセージ表示=有り、暗号通信禁止=無し、デバイス鍵識別=3の受信機に対してメッセージ番号=3のメッセージを表示する、が記憶される。つまり、ICカード26は受信機2に対して、これら情報を送信する。これら情報を受信した受信機2は、メッセージ番号=3のメッセージを放送局から分離し、画像もしくは音声信号への変換部31にて表示画面を生成し、多重処理部32にてTV信号に多重する。

【0072】この図15の例では、メッセージ表示=有り、暗号通信禁止=無しであり、当該受信機が不良受信機に指定されている。あるいはサービスセンターに連絡が必要などのメッセージ表示がなされる。しかしながら、暗号通信は禁止されておらず、契約があればスクランブル放送の視聴は可能である。メッセージ表示=有り、暗号通信禁止=有り、にすれば、メッセージ表示をおこない、さらに暗号通信を禁止し、視聴不可とすることもできる。

【0073】このように、放送側からメッセージ表示情報と暗号通信禁情報とをそれぞれ設定することにより、不良受信機に対する不正防止処理の自由度を広げることができる。

【0074】なお、上記説明した第2の実施形態に係る放送受信処理システムにおける不正防止処理の基本的な処理の流れは、図9に示すフローチャートで示した通りである。異なる点は鍵の暗号化処理及び復号化処理だけである。つまり、第1の実施形態では、ICカード内でデバイス鍵によりスクランブル鍵が暗号化され、ICカードから受信機に対して暗号化されたスクランブル鍵が送信され、受信機内でデバイス鍵により暗号化されたスクランブル鍵が復号化される。これに対して、第2の実施形態では、ICカード内でデバイス鍵によりセッション鍵が暗号化され、さらにセッション鍵によりスクランブル鍵が暗号化され、ICカードから受信機に対して暗号化されたセッション鍵及び暗号化されたスクランブル鍵が送信され、受信機内でデバイス鍵により暗号化され

たセッション鍵が復号化され、セッション鍵により暗号化されたスクランブル鍵が復号化される。

【0075】以下、上記説明したこの発明の作用効果についてまとめる。

【0076】(1) 放送局側が I Cカードに対し、不正が行われている受信機と暗号通信しないように指定できる。つまり、第1の実施形態では、不正が行われている受信機に対して、I Cカードは暗号化されたスクランブル鍵を提供しない。或いは、第2の実施形態では、不正が行われている受信機に対して、I Cカードは暗号

化されたセッション鍵及びスクランブル鍵を提供しない。

【0077】(2) 放送局側が I Cカードに対して指示を出すことにより、不正が行われている受信機に所定のメッセージを表示させることができる。つまり、I Cカードは、不正がおこなわれている受信機に対してメッセージ出力制御情報を出力する。

【0078】(3) 放送局側が、不正が行われている受信機と I Cカードとの暗号通信を規制したり、不正が行われている受信機に所定のメッセージを表示させたりすることが、選択的に指定できる。つまり、第1の実施形態では、放送局側が、不正が行われている受信機に対する暗号化されたスクランブル鍵の送信を規制したり、不正が行われている受信機に対してメッセージ出力制御情報を出力してメッセージを表示させたりすることが、選択的に指定できる。また、第2の実施形態では、放送局側が、不正が行われている受信機に対する暗号化されたセッション鍵及び暗号化されたスクランブル鍵の送信を規制したり、不正が行われている受信機に対してメッセージ出力制御情報を出力してメッセージを表示させたりすることが、選択的に指定できる。

【0079】なお、本願発明は、上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせることでよく、その場合組み合わせた効果が得られる。更に、上記実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば、実施形態に示される全構成要件からいくつもの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題が解決でき、発明の効果の欄で述べられている効果が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【0080】

【発明の効果】この発明によれば、特定機種の受信装置だけをターゲットにして不正を防止することが可能な放送受信処理システム、放送受信処理方法、及び受信装置に適用される I Cカードを提供できる。

【図面の簡単な説明】

【図1】この発明の第1の実施形態に係る放送受信処理システムの一例の基本構成を示す図である。

【図2】図1に示す放送受信処理システムに適用される受信機及び I Cカードの動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにして I Cカードとの暗号通信を禁止する不正防止処理の第1例を説明するための図である。

【図3】図1に示す放送受信処理システムに適用される受信機及び I Cカードの動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにして I Cカードとの暗号通信を禁止する不正防止処理の第2例を説明するための図である。

【図4】図1に示す放送受信処理システムに適用される放送局の動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにして I Cカードとの暗号通信を禁止する不正防止処理の第1例及び第2例を説明するための図である。

【図5】図1に示す放送受信処理システムに適用される受信機及び I Cカードの動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにして所定のメッセージを表示させる不正防止処理を説明するための図である。

【図6】図1に示す放送受信処理システムに適用される放送局の動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにして所定のメッセージを表示させる不正防止処理を説明するための図である。

【図7】図1に示す放送受信処理システムに適用される放送局の動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにして I Cカードとの暗号通信を選択的に禁止したり、特定機種の受信装置だけをターゲットにして所定のメッセージを選択的に表示させたりする不正防止処理を説明するための図である。

【図8】図1に示す放送受信処理システムに適用される受信機及び I Cカードの動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにして I Cカードとの暗号通信を選択的に禁止したり、特定機種の受信装置だけをターゲットにして所定のメッセージを選択的に表示させたりする不正防止処理を説明するための図である。

【図9】特定機種の受信機だけをターゲットにして、I Cカードとの暗号通信を禁止する不正防止処理を説明するフローチャートである。

【図10】特定機種の受信機だけをターゲットにして、所定のメッセージの表示を指示する不正防止処理を説明するフローチャートである。

【図11】特定機種の受信機だけをターゲットにして、I Cカードとの暗号通信を選択的に禁止したり、選択的に所定のメッセージを表示させたりする不正防止処理を説明するフローチャートである。

【図12】この発明の第2の実施形態に係る放送受信処理システムの一例の基本構成を示す図である。

【図13】図12に示す放送受信処理システムに適用される受信機及びICカードの動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにしてICカードとの暗号通信を禁止する不正防止処理の第2例を説明するための図である。

【図14】図12に示す放送受信処理システムに適用される受信機及びICカードの動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにして所定のメッセージを表示させる不正防止処理を説明するための図である。

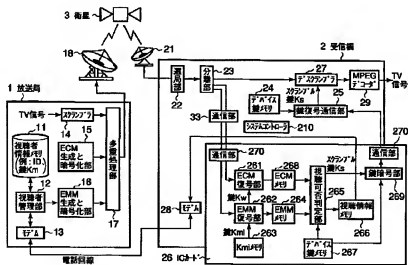
【図15】図12に示す放送受信処理システムに適用される受信機及びICカードの動作説明を補足するため図であり、特に、特定機種の受信装置だけをターゲットにしてICカードとの暗号通信を選択的に禁止したり、特定機種の受信装置だけをターゲットにして所定のメッセージを選択的に表示させたりする不正防止処理を説明するための図である。

【符号の説明】

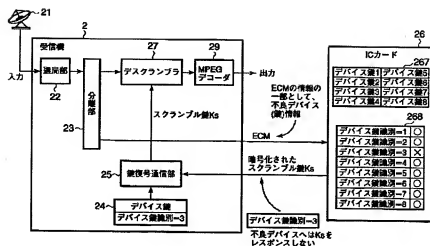
- 1…放送局
- 2…受信装置
- 3…衛星
- 11…視聴者情報メモリ
- 12…視聴者管理部
- 13…モデム
- 14…スクランブラ

- * 15…ECM生成と暗号化部
- 15a…ECM生成部
- 15b…暗号化部
- 16…ECM生成と暗号化部
- 16a…ECM生成部
- 16b…暗号化部
- 17…多重処理部
- 18…アンテナ
- 19…メッセージ生成部
- 20 21…アンテナ
- 22…選局部
- 23…分離部
- 24…デバイス鍵メモリ
- 25…鍵復号通信部
- 26…ICカード
- 27…デスクランブラ
- 28…モデム
- 29…MPEGデコーダ
- 261…ECM復号部
- 262…ECM復号部
- 263…Kmiメモリ
- 264…ECMメモリ
- 265…視聴可否判定部
- 266…視聴情報メモリ
- 267…デバイス鍵メモリ
- 268…ECMメモリ
- * 271…セッション鍵生成部

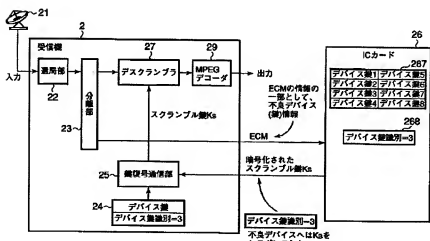
【図1】



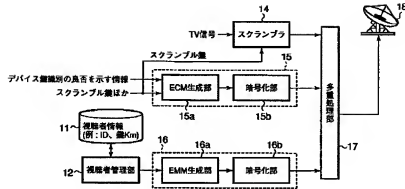
【図2】



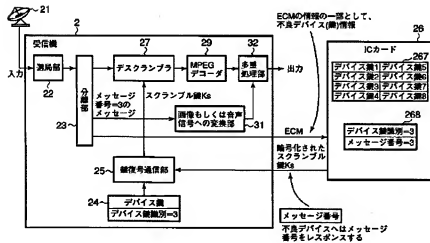
【図3】



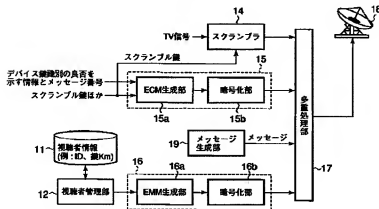
【図4】



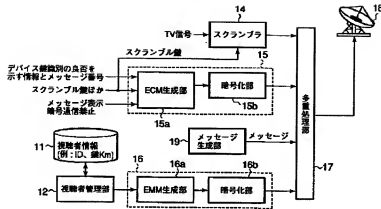
【図5】



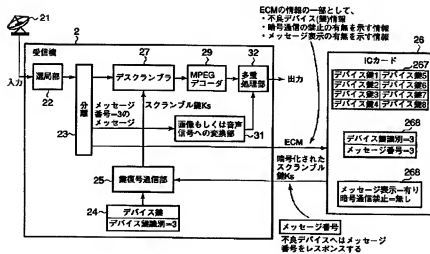
【図6】



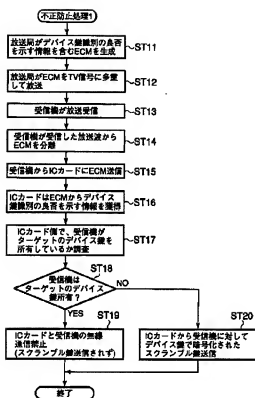
【図7】



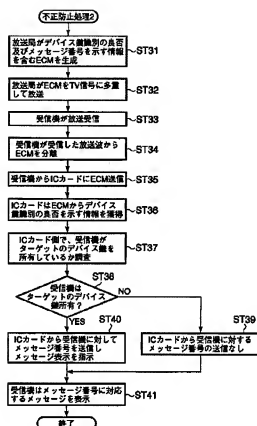
【図8】



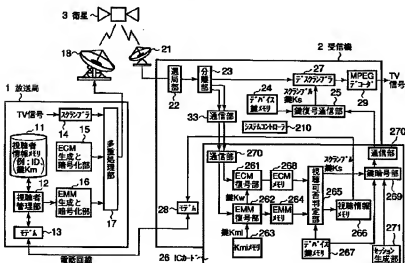
【図9】



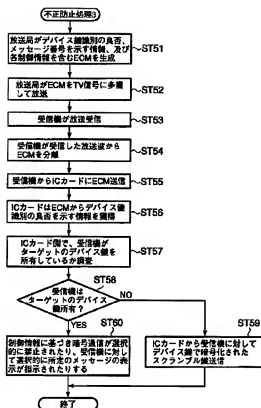
【図10】



【図12】



【図11】



【図13】

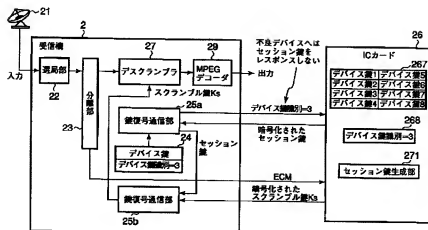


Figure 1 is a block diagram of a video transmission system. The system includes an antenna 21, a receiving section 22, a public line section 23, a descrambler 27, a scrambling key 29, an MPEG decoder 32, and an output section 31. It also features a message box 24, a session ID 25, a device ID 26, and a session ID 27. The system is designed to receive and decode encrypted video data, including scrambling keys and session information, to output the original video content.

[illegible]

(51) Int. Cl. ⁷	識別記号	F I	7-73-1' (参考)
H 0 4 L 9/18		H 0 4 L 9/00	6 5 1
H 0 4 N 5/44		G 0 6 K 19/00	R
7/173	6 4 0		Q
		H 0 4 L 9/00	6 0 1 A

F ターム(参考) 5B035 AA13 BB09 BC00
5C025 CA02 CA09 CA18 CB07 DA01
DA04
5C064 BA01 BB02 BC06 BC22 BC23
BD03 BD08 BD09 BD16 CA14
CB01 CB08 CC02 CC04
5J104 AA12 EA02 NA02 NA35 PA05
PA06

SPECIFICATION <EXCERPT>

[0054] Next, the second embodiment according to the present invention is described with reference to the drawings. This second embodiment is an application of the first embodiment as described above. Therefore, the same descriptions as in the first embodiment are not repeated.

[0055] FIG. 12 is a base block diagram of the broadcast-reception processing system according to the second embodiment of the present invention. FIG. 13 to FIG. 15 illustrates an anti-abuse process of preventing a computer abuse only for a specific type of the receiver (malicious receiver) in the broadcast-reception processing system as described in FIG. 12. The anti-abuse process shown in FIG. 13 corresponds to the one shown in FIG. 3, the anti-abuse process shown in FIG. 14 corresponds to the one shown in FIG. 5, the anti-abuse process shown in FIG. 15 corresponds to the one shown in FIG. 8. The following describes the broadcast-reception processing systems shown in FIG. 12 to FIG. 15, in particular, differences from the ones shown in FIG. 1, FIG. 3, FIG. 5, and FIG. 8.

[0056] Initially, the receiver 1 and the IC card 2 authenticate each other using cryptographic communication. When the mutual authentication succeeds, a temporary session key is provided from the IC card 2 to the receiver 1. This temporary session key is generated by the IC card 2 for the current mutual authentication, and another key is generated by the IC card 2 for the next mutual authentication.

[0057] First, the receiver 1 provides a device-key identification number to the IC card 2. In the case where the IC card 2 has received the ECM without the device-key identification

number indicating that the receiver is malicious so that the memory 268 in the IC card 2 contains no information indicating that the receiver is malicious, the IC card 2 i) generates the temporary session key in the session key generating unit 271, ii) encrypts the generated session key using the device key of the receiver, and iii) passes the encrypted session key to the receiver 1. It is noted that the session-key generating unit 271 uses a cryptography processing unit, a random number generator, and the like to avoid generating the identical session key. In this manner, the session key is passed only to the receiver having the correct device key because the session key is encrypted using the device key. Moreover, the previous session key cannot be used again because the session key changes for each mutual authentication. Thus, as described in the first embodiment, this system has higher security than the system where the scramble key is encrypted using the device key. The receiver 2 shares the session key with the IC card 26. Then, upon receiving ECM, the receiver 1 provides the received ECM to the IC card 26. In response to this, the receiver 1 obtains the scramble key encrypted with the session key. Then, this key is decrypted in the key decrypting communication unit 25b, and the decrypted key is provided to the descrambling unit 27. It is noted that device key identification indicating the malicious device is appropriately transmitted to the ECM from the broadcasting station. Thus, upon receiving this identification, the IC card 26 stores the received identification in the memory 268 and, from the next mutual authentication, the cryptographic communication using the stored device key identification is not performed so as to prevent the session key from being shared. On the contrast, when the troubled receiver 2 does not need to be restricted anymore due to an upgrade or the like, the broadcasting side transmits the device key identification of the receiver to be derestricted, and the IC card 2 deletes this identification from the memory 268 in the case where

the memory 268 stores this device key identification.

[0058] For example, in the receiver 2, the mutual authentication (decrypting process for the session key) is performed in the key decrypting communication unit 25a, and the scramble key is decrypted in the key decrypting communication unit 25b. Alternatively, when using the same algorithm, the decrypting process may be commoditized for the session key and the scramble key as long as the decrypting process has the structure where one key is changed over the other key.

[0059] The following summarizes the key coding process and the key decrypting process. In particular, the following sections summarize a process after finding from the IC card 26 that the receiver 2 into which this IC card 26 is inserted does not match any of the receivers to be eliminated.

[0060] As shown in FIG. 12, the IC card 26 includes the session key generating unit 271. The session key generated from this session-key generating unit 271 is provided to the key encrypting unit 269. In addition, the key encrypting unit 269 receives the device key identical to the device key stored in the target receiver 2 among the multiple device keys stored in the device key memory 267. The key encrypting unit 269 also receives the scramble key contained in the ECM stored in the ECM memory 268.

[0061] The key encrypting unit 269 encrypts the session key using the device key, and encrypts the scramble key using the session key. The session and scramble keys encrypted by the key encrypting unit 269 are provided to the receiver 2 via the communication unit 270. The receiver 2 receives the encrypted session key and the encrypted scramble key via the key decrypting communication unit 25. It is noted that part of the key decrypting communication unit 25 corresponds to the key decrypting communication unit 25a as shown in FIG. 13, part of the key

decrypting communication unit 25 corresponds to the key decrypting communication unit 25b as shown in FIG. 13 as well.

[0062] The key decrypting communication unit 25 decrypts the encrypted session key using the device key provided from the device key memory 24. The key decrypting communication unit 25 also decrypts the encrypted scramble key using the decrypted session key, and then provides the decrypted scramble key to the descrambling unit 27. The descrambling unit 27 descrambles the broadcasting data using the provided scramble key.

[0063] With reference to FIG. 14, the next section describes a message notifying process of notifying the message only for the specific type of the receiver (malicious receiver) in the broadcast-reception processing system as illustrated in FIG. 12. FIG. 14 illustrates a schematic block diagram for the receiver 2 and the IC card 26. The base structure of the receiver 2 and the IC card 26 shown in FIG. 14 is the same as the one shown in FIG. 12. However, as shown in FIG. 14, a data-to-image-or-audio-signal converter 31 and a multiplexer 32 are added to this receiver 2.

[0064] It is assumed that, as the method for identifying the malicious receiver, this system employs a method of multiplexing, into the ECM, a device-key identification table indicating whether or not the receiver is malicious, or a method of multiplexing only the device key identification of the malicious receiver into the ECM, as described in FIG. 3 (or FIG. 13).

[0065] In FIG. 14, the broadcast side transmits the information on the device key identification to identify the malicious receiver and the information indicating a message number to be displayed on the receiver having the device key identification. The receiver 2 receives the above information and then provides it to the IC card 26. The IC card 26 stores the provided information in the ECM memory 268. The IC card 26 also notifies, of the message output-control information, the receiver having the device key

indicated as a malicious receiver by the device key identification. The message output-control information is the message number for example.

[0066] In the example of FIG. 14, the IC card 26 connected to the receiver 2 with device key identification = 3 stores the device key identification of the receiver 2 in the ECM memory 268, and then notifies the receiver of the message number stored in the ECM memory 268 to request a display of the message number.

[0067] Upon notifying of the message number, the receiver 2 causes the demultiplexing unit 23 to demultiplex the ECM to obtain the message for the requested message number. This data is, for example, character data for displaying the message. The obtained message information is converted into the image signal to display on TV by the data-to-image-or-audio-signal converter 31, and the multiplexing process for a on-screen display is performed by the multiplexer 32. It is noted that the on-screen display of the character is described here as an example, however, a voice or an image may be used. The point is that the broadcasting station can specify the message to be displayed for the specific type of the receiver. In this manner, each of the receiver can receive a different message such as "repairing is required" or "inform the owner of the contact information", and thereby the owner can know the message. The above-mentioned message which is placed on the service information of the digital broadcasting for example can be transmitted.

[0068] In the above example, for the malicious receiver, the broadcasting station specifies to prohibit the cryptographic communication and stop providing of the scramble key or to have the receiver display the message. With reference to FIG. 15, the next section describes another example where the broadcasting station can selectively specify to prohibit the cryptographic communication (non-transmission of the encrypted session key and

the encrypted scramble key) and to display the message (transmission of the message output-control information).

[0069] The broadcasting station 1 acts on the malicious receiver as follows: i) specify to prohibit the cryptographic communication and to display the message, ii) specify to prohibit the cryptographic communication and not to display the message, iii) specify not to prohibit the cryptographic communication and to display the message, and iv) specify not to prohibit the cryptographic communication and not to display the message.

[0070] FIG. 15 is a diagram illustrating an example of the receiver 2 and the IC card 26 which receive the broadcast wave transmitted from the broadcasting station 1. The base structure of the receiver 2 and the IC card 26 shown in FIG. 15 is the same as the one shown in FIG. 14. They are different in that the IC card 26 shown in FIG. 15 stores two pieces of information, i.e. the information indicating whether or not the cryptographic communication is prohibited and the information indicating whether or not the message is displayed. These two pieces of information are inputted into the IC card 26 as a part of the ECM. For the malicious receiver, the cryptographic communication and the display instructions are controlled based on the two pieces of information.

[0071] For example, in FIG. 15, the ECM memory 268 stores i) message display = applicable, ii) cryptographic-communication prohibition = not applicable, and iii) displaying the message of message number = 3 for the receiver having device key identification = 3. More specifically, the IC card 26 transmits the above information to the receiver 2, and upon receiving the information, the receiver 2 demultiplexes the broadcast signal to obtain the message of message number = 3. Then, the on-screen display for the obtained message is generated by the data-to-image-or-audio signal converter 31, and the generated on-screen display data is multiplexed into the TV signal by the

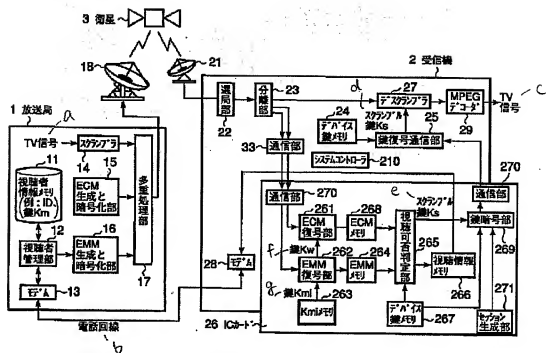
multiplexer 32.

[0072] The example of FIG. 15 is under the condition of message display = applicable and cryptographic communication prohibition = not applicable, and thus the message such as "this receiver is assigned to the malicious receiver" or "need to contact the service center" is displayed. However, it is possible for a subscriber to view the scrambled broadcasting because the cryptographic communication is not prohibited. Under the condition of message display = applicable and cryptographic-communication prohibition = applicable, the message can be displayed, and the cryptographic communication can be prohibited to disable the viewing of the scrambled broadcasting as well.

[0073] In this manner, the anti-abuse process for the malicious receiver is made more flexible by setting each of the message-display information and the cryptographic-communication prohibition information from the broadcast side.

DRAWINGS

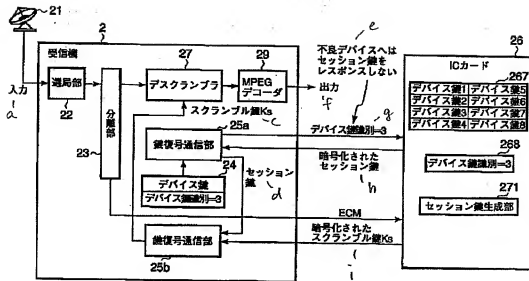
FIG. 12



- 1: Broadcasting station
- 2: Receiver
- 3: Satellite
- 11: Viewer information memory (such as ID, key Km)
- 12: Viewer management unit
- 13: Modem
- 14: Scrambling unit
- 15: ECM generating and encrypting unit
- 16: EMM generating and encrypting unit
- 17: Multiplexing unit
- 22: Station selector
- 23: Demultiplexing unit
- 24: Device key memory
- 25: Key decrypting communication unit
- 26: IC card
- 27: Descrambling unit

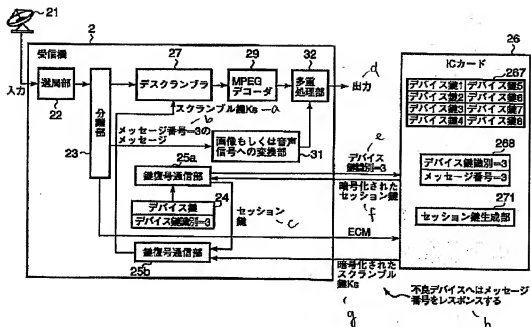
28: Modem
29: MPEG decoder
33: Communication unit
210: System controller
261: ECM decrypting unit
262: EMM decrypting unit
263: Kmi memory
264: EMM memory
265: Viewing determination unit
266: Viewing information memory
267: Device key memory
268: ECM memory
269: Key encrypting unit
270: Communication unit
271: Session generating unit
a, c: TV signal
b: Phone line
d, e: Scramble key K_s
f: Key K_w
g: Key K_{mi}

FIG. 13



- 2: Receiver
- 22: Station selector
- 23: Demultiplexing unit
- 24: Device key, Device key identification = 3
- 25a, 25b: Key decrypting communication unit
- 26: IC card
- 27: Descrambling unit
- 29: MPEG decoder
- 267: Device keys 1 to 8
- 268: Device key identification = 3
- 271: Session generating unit
- a: Input
- c: Scramble key Ks
- d: Session key
- e: Not return the session key to the malicious device
- f: Output
- g: Device key identification = 3
- h: Encrypted session key
- i: Encrypted scramble key Ks

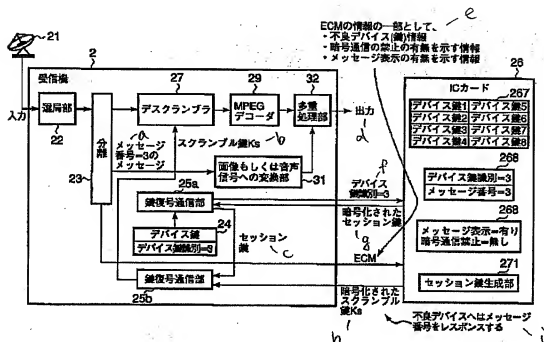
FIG. 14



- 2: Receiver
- 22: Station selector
- 23: Demultiplexing unit
- 24: Device key, Device key identification = 3
- 25a, 25b: Key decrypting communication unit
- 26: IC card
- 27: Descrambling unit
- 29: MPEG decoder
- 31: Data-to-image-or-audio-signal converter
- 32: Multiplexer
- 267: Device keys 1 to 8
- 268: Device key identification = 3, Message number = 3
- 271: Session generating unit
- a: Scramble key Ks
- b: Message of message number = 3
- c: Session key
- d: Output
- e: Device key identification = 3

- f: Encrypted session key
 g: Encrypted scramble key Ks
 h: Return the message number to the malicious device

FIG. 15



- 2: Receiver
 22: Station selector
 23: Demultiplexing unit
 24: Device key, Device key identification = 3
 25a, 25b: Key decrypting communication unit
 26: IC card
 27: Descrambling unit
 29: MPEG decoder
 31: Data-to-image-or-audio-signal converter
 32: Multiplexer
 267: Device keys 1 to 8
 268: Device key identification = 3, Message number = 3
 268: Message display = applicable, Cryptographic-communication

prohibition = not applicable

271: Session generating unit

a: Message of message number = 3

b: Scramble key K_s

c: Session key

d: Output

e: As a part of the ECM, i) malicious device (key) information, ii) information indicating whether or not the cryptographic communication is prohibited, and iii) information indicating whether or not the message is displayed

f: Device key identification = 3

g: Encrypted session key

h: Encrypted scramble key K_s

i: Return the message number to the malicious device